<u>IN THE CLAIMS</u>:

1. (Original) An elliptic curve arithmetic operation device for performing one of an addition and a doubling on an elliptic curve *E*: $y \{ 2=f(x)$ on a residue class ring of polynomials in two variables α and β, moduli of the residue class ring being polynomials $\beta \{ 2\text{-}f(\alpha)$ and $h(\alpha)$, where $f(\alpha)=\alpha \{ 3+a\alpha+b$, a and b are constants, and $h(\alpha)$ is a polynomial in the variable α, the elliptic curve arithmetic operation device comprising:

acquiring means for acquiring affine coordinates of at least one point on the elliptic curve *E* and operation information indicating one of the addition and the doubling, from an external source;

transforming means for performing a coordinate transformation on the acquired affine coordinates to generate Jacobian coordinates, the coordinate transformation being transforming affine coordinates $(\phi\ (\alpha),\ \beta x\varphi,(\alpha))$ of a given point on the elliptic curve *E* using polynomials

$$X(\alpha)=f(\alpha)\ x\phi\ (\alpha)$$

$$Y(\alpha)=f(\alpha)\ \ \{ 2x\varphi\ (\alpha)$$

$$Z(\alpha)=1$$

into Jacobian coordinates $(X(\alpha)\ :Y(\alpha)\ :\ \beta xZ(\alpha))$, $\phi\ (\alpha)$ and $\varphi\ (\alpha)$ being polynomials; and

operating means for performing one of the addition and the doubling indicated by the acquired operation information, on the generated Jacobian coordinates to obtain Jacobian coordinates of a point on the elliptic curve *E*.

2. (Original) The elliptic curve arithmetic operation device of Claim 1,

wherein the acquiring means

(a) in a first case acquires affine coordinates of two different points on the elliptic curve E and operation information indicating the addition, and

(b) in a second case acquires affine coordinates of a single point on the elliptic curve E and operation information indicating the doubling,

wherein the transforming means

(a) in the first case performs the coordinate transformation on the acquired affine coordinates of the two different points to generate Jacobian coordinates of the two different points, and

(b) in the second case performs the coordinate transformation on the acquired affine coordinates of the single point to generate Jacobian coordinates of the single point, and

wherein the operating means

(a) in the first case performs the addition indicated by the acquired operation information on the generated Jacobian coordinates of the two different points to obtain the Jacobian coordinates of the point on the elliptic curve E, and

(b) in the second case performs the doubling indicated by the acquired operation information on the generated Jacobian coordinates of the single point to obtain the Jacobian coordinates of the point on the elliptic curve E.

3. (Currently Amended) The elliptic curve arithmetic operation device of Claim 2,

wherein in the first case

the acquiring means acquires affine coordinates

$\cancel{(X1(\alpha), \beta x Y1(\alpha))}$ $\underline{(\phi_1(\alpha), \beta x \varphi_1(\alpha))}$

$\cancel{(X2(\alpha), \beta x Y2\ (\alpha))}$ $\underline{(\phi_2\ (\alpha), \beta x \varphi_2(\alpha))}$

of the two different points on the elliptic curve E and the operation information indicating the addition,

the transforming means performs the coordinate transformation on the acquired affine coordinates of the two different points to generate Jacobian coordinates

$$(X1(\alpha) : Y1(\alpha) : \beta x Z1(\alpha))$$

$$(X2(\alpha) : Y2(\alpha) : \beta x Z2\ (\alpha))$$

of the two different points, and

the operating means computes

$$U1(\alpha) = X1(\alpha)\ xZ2(\alpha)\ \{ 2$$

$$U2(\alpha) = X2(\alpha)\ xZ1(\alpha)\ \{ 2$$

$$S1(\alpha) = Y1(\alpha)\ xZ2(\alpha)\ \{ 3$$

$$S2(\alpha) = Y2(\alpha)\ xZ1(\alpha)\ \{ 3$$

$$H(\alpha) = U2(\alpha) - U1(\alpha)$$

$$r(\alpha) = S2(\alpha) - S1(\alpha)$$

and computes

$$X3(\alpha) = -H(\alpha)\ \{ 3-2xU1(\alpha)xH(\alpha)\ \{\ 2+r(\alpha)\ \{ 2$$

$$Y3(\alpha) = -S1(\alpha)\ xH(\alpha)\ \{ 3+r\ (\alpha)\ x\ (U1(\alpha)xH(\alpha)\ \{ 2-X3\ (\alpha))$$

$$Z3(\alpha) = Z1(\alpha)\ xZ2(\alpha)\ xH(\alpha)$$

to obtain Jacobian coordinates $(X3(\alpha) : Y3(\alpha) : \beta x Z3(\alpha)$ of the point on the elliptic curve E.

4. (Currently Amended) The elliptic curve arithmetic operation device of Claim 2, wherein in the second case

the acquiring means acquires affine coordinates

$$\cancel{(X1(\alpha), \beta x Y1(\alpha))}\ \underline{(\phi_1 (\alpha), \beta x \varphi_1(\alpha))}$$

of the single point on the elliptic curve *E* and the operation information indicating the doubling,

the transforming means performs the coordinate transformation on the acquired affine coordinates of the single point to generate Jacobian coordinates

$$(X1(\alpha) : Y1(\alpha) : \beta x Z1(\alpha))$$

of the single point, and

the operating means computes

$$S(\alpha)=4\,x X1(\alpha) x Y1(\alpha)\ \{ 2$$

$$M(\alpha)=3x X1(\alpha)\ \{ 2+\alpha x Zl(\alpha)\ \{ 4x f(\alpha)\ \{ 2$$

$$T(\alpha)=-2x S(\alpha)+M(\alpha)\ \{ 2$$

and computes

$$X3(\alpha)=T(\alpha)$$

$$Y3(\alpha)=-8x Y1(\alpha)\ \{ 4+M(\alpha) x (S(\alpha)-T(\alpha))$$

$$Z3(\alpha)=2x Y1(\alpha) x Z1(\alpha)$$

to obtain Jacobian coordinates $(X3(\alpha) : Y3(\alpha) : \beta x Z3(\alpha))$ of the point on the elliptic curve *E*.

5. (Currently Amended) The elliptic curve arithmetic operation device of Claim 2, wherein the acquiring means

(a) in the first case acquires affine coordinates

~~$(X1(\alpha), \beta xY1(\alpha))$~~ $\underline{(\phi_1(\alpha), \beta x\varphi_1(\alpha))}$

~~$(X2(\alpha), \beta xY2(\alpha))$~~ $\underline{(\phi_2(\alpha), \beta x\varphi_2(\alpha))}$

of the two different points on the elliptic curve E and the operation information indicating the addition, and

(b) in the second case acquires affine coordinates

~~$(X1(\alpha), \beta xY1(\alpha))$~~ $\underline{(\phi_1(\alpha), \beta x\varphi_1(\alpha))}$

of the single point on the elliptic curve E and the operation information indicating the doubling,

wherein the transforming means

(a) in the first case performs the coordinate transformation on the acquired affine coordinates of the two different points to generate Jacobian coordinates

$(X1(\alpha) : Y1(\alpha) : \beta xZ1(\alpha))$

$(X2(\alpha) : Y2(\alpha) : \beta xZ2(\alpha))$

of the two different points, and

(b) in the second case performs the coordinate transformation on the acquired affine coordinates of the single point to generate Jacobian coordinates

$(X1(\alpha) : Y1(\alpha) : \beta xZ1(\alpha))$

of the single point, and

wherein the operating means

(a) in the first case computes

$$U1(\alpha) = X1(\alpha)xZ2(\alpha) \ \{ \ 2$$

$$U2(\alpha) = X2(\alpha)xZ1(\alpha) \ \{ \ 2$$

$$S1(\alpha) = Y1(\alpha)xZ2(\alpha) \ \{ \ 3$$

$$S2(\alpha) = Y2(\alpha)xZ1(\alpha) \ \{ \ 3$$

$$H(\alpha) = U2(\alpha) - U1(\alpha)$$

$$r(\alpha) = S2(\alpha) - S1(\alpha)$$

and computes

$$X3(\alpha) = -H(\alpha) \ \{ \ 3-2xU1(\alpha)xH(\alpha) \ \{ \ 2+r(\alpha) \ \{ \ 2$$

$$Y3(\alpha) = -S1(\alpha)xH(\alpha) \ \{ \ 3+r(\alpha)x(U1(\alpha)xH(\alpha) \ \{ \ 2-X3(\alpha))$$

$$Z3(\alpha) = Z1(\alpha) xZ2(\alpha)xH(\alpha)$$

to obtain Jacobian coordinates $(X3(\alpha) : Y3(\alpha) : \beta xZ3(\alpha))$ of the point on the elliptic curve *E*, and

(b) in the second case computes

$$S(\alpha) = 4xX1(\alpha)xY1(\alpha) \ \{ \ 2$$

$$M(\alpha) = 3xX1(\alpha) \ \{ \ 2+axZ1(\alpha) \ \{ \ 4xf(\alpha) \ \{ \ 2$$

$$T(\alpha) = -2xS(\alpha)+M(\alpha) \ \{ \ 2$$

and computes

$$X3(\alpha) = T(\alpha)$$

$$Y3(\alpha) = -8xYl(\alpha) \ \{ \ 4 + M(\alpha)x(S(\alpha) - T(\alpha))$$

$$Z3(\alpha) = 2xY1(\alpha)xZ1(\alpha)$$

to obtain the Jacobian coordinates $(X3(\alpha) : Y3(\alpha) : \beta xZ3(\alpha))$ of the point on the elliptic curve *E*.

6. (Original) An elliptic curve order computation device for computing an order of an elliptic curve according to a Schoof-Elkies-Atkin algorithm, comprising the elliptic curve arithmetic operation device of Claim 1.

7. (Original) The elliptic curve order computation device of Claim 6 comprising the elliptic curve arithmetic operation device of Claim 2.

8. (Original) The elliptic curve order computation device of Claim 7 comprising the elliptic curve arithmetic operation device of Claim 5.

9-22. (Cancelled)

23. (Currently Amended) An elliptic curve arithmetic operation method used in an elliptic curve arithmetic operation device equipped with an acquiring means, a transforming means, and an operating means, for performing one of an addition and a doubling on an elliptic curve $E: y \{ 2=f(x)$ on a residue class ring of polynomials in two variables α and β, moduli of the residue class ring being polynomials $\beta \{ 2-f(\alpha)$ and $h(\alpha)$, where $f(\alpha)=\alpha \{ 3+a\alpha+b$, a and b are constants, and $h(\alpha)$ is a polynomial in the variable α, the elliptic curve arithmetic operation method comprising:

an acquiring step performed by the acquiring means, for acquiring affine coordinates of at least one point on the elliptic curve E and operation information indicating one of the addition and the doubling, from an external source;

a transforming step performed by the transforming means, for performing a coordinate transformation on the acquired affine coordinates to generate Jacobian coordinates,

the coordinate transformation being transforming affine coordinates $(\phi\ (\alpha),\ \beta x\varphi(\alpha))$ of a given point on the elliptic curve E using polynomials

$$X(\alpha) = f(\alpha) x \phi\ (\alpha)$$

$$Y(\alpha) = f(\alpha)\ \{\ 2x\varphi\ (\alpha)$$

$$Z(\alpha) = 1$$

into Jacobian coordinates $(X(\alpha)\ {:}Y(\alpha)\ {:}\beta x Z(\alpha))$, $\phi\ (\alpha)$ and $\cancel{\phi\ (\alpha)}$ $\underline{\varphi(\alpha)}$ being polynomials; and

an operating step performed by the operating means, for performing one of the addition and the doubling indicated by the acquired operation information, on the generated Jacobian coordinates to obtain Jacobian coordinates of a point on the elliptic curve E.

24. (Cancelled)

25. (Original) A computer-readable storage medium storing an elliptic curve arithmetic operation program used in an elliptic curve arithmetic operation device equipped with acquiring means, transforming means, and operating means, for performing one of an addition and a doubling on an elliptic curve $E{:}\ y\ \{\ 2{=}f(x)$ on a residue class ring of polynomials in two variables α and β, moduli of the residue class ring being polynomials $\beta\ \ \{\ 2\text{-}f(\alpha)$ and $h(\alpha)$, where $f(\alpha) = \alpha\ \{\ 3 + a\alpha + b$, a and b are constants, and $h(\alpha)$ is a polynomial in the variable α, the elliptic curve arithmetic operation program comprising:

an acquiring step performed by the acquiring means, for acquiring affine coordinates of at least one point on the elliptic curve E and operation information indicating one of the addition and the doubling, from an external source;

a transforming step performed by the transforming means, for performing a coordinate transformation on the acquired affine coordinates to generate Jacobian coordinates, the coordinate transformation being transforming affine coordinates $(\phi(\alpha), \beta x \varphi(\alpha))$ of a given point on the elliptic curve *E* using polynomials

$$X(\alpha) = f(\alpha) x \phi(\alpha)$$

$$Y(\alpha) = f(\alpha) \{ 2x\varphi(\alpha)$$

$$Z(\alpha) = 1$$

into Jacobian coordinates $(X(\alpha) : Y(\alpha) : \beta x Z(\alpha))$, $\phi(\alpha)$ and $\varphi(\alpha)$ being polynomials; and

an operating step performed by the operating means, for performing one of the addition and the doubling indicated by the acquired operation information, on the generated Jacobian coordinates to obtain Jacobian coordinates of a point on the elliptic curve *E*.

26. (Original) The storage medium of Claim 25, wherein the acquiring step

(a) in a first case acquires affine coordinates of two different points on the elliptic curve *E* and operation information indicating the addition, and

(b) in a second case acquires affine coordinates of a single point on the elliptic curve *E* and operation information indicating the doubling,

wherein the transforming step

(a) in the first case performs the coordinate transformation on the acquired affine coordinates of the two different points to generate Jacobian coordinates of the two different points, and

(b) in the second case performs the coordinate transformation on the acquired affine coordinates of the single point to generate Jacobian coordinates of the single point, and

wherein the operating step

(a) in the first case performs the addition indicated by the acquired operation information on the generated Jacobian coordinates of the two different points to obtain the Jacobian coordinates of the point on the elliptic curve *E*, and

(b) in the second case performs the doubling indicated by the acquired operation information on the generated Jacobian coordinates of the single point to obtain the Jacobian coordinates of the point on the elliptic curve *E*.

27. (Currently Amended) The storage medium of Claim 26, wherein in the first case the acquiring step acquires affine coordinates

$$\cancel{(X1(\alpha), \beta x Y1(\alpha))}\ \underline{(\phi_1 (\alpha), \beta x \varphi_1(\alpha))}$$

$$\cancel{(X2(\alpha), \beta x Y2(\alpha))}\ \underline{(\phi_2 (\alpha), \beta x \varphi_2(\alpha))}$$

of the two different points on the elliptic curve E and the operation information indicating the addition,

the transforming step performs the coordinate transformation on the acquired affine coordinates of the two different points to generate Jacobian coordinates

$$(X1(\alpha) : Y1(\alpha) : \beta x Z1(\alpha))$$

$$(X2(\alpha) : Y2(\alpha) : \beta x Z2(\alpha))$$

of the two different points, and

the operating step computes

$$U1(\alpha) = X1(\alpha) x Z2(\alpha) \{ 2$$

$$U2(\alpha) = X2(\alpha) x Z1(\alpha) \{ 2$$

$$S1(\alpha) = Y1(\alpha) x Z2(\alpha) \{ 3$$

$$S2(\alpha) = Y2(\alpha) x Z1(\alpha) \{ 3$$

$$H(\alpha) = U2(\alpha) - U1(\alpha)$$

$$r(\alpha) = S2(\alpha) - S1(\alpha)$$

and computes

$$X3(\alpha) = -H(\alpha)\ \{\ 3 - 2xU1(\alpha)xH(\alpha)\ \{\ 2 + r(\alpha)\ \{\ 2$$

$$Y3(\alpha) = -S1(\alpha)xH(\alpha)\ \{\ 3 + r(\alpha)x(U1(\alpha)xH(\alpha)\ \{\ 2 - X3(\alpha))$$

$$Z3(\alpha) = Z1(\alpha)xZ2(\alpha)xH(\alpha)$$

to obtain Jacobian coordinates $(X3(\alpha) : Y3(\alpha) : \beta xZ3(\alpha))$ of the point on the elliptic curve E.

28. (Currently Amended) The storage medium of Claim 26,

wherein in the second case the acquiring step acquires affine coordinates

$$\cancel{(X1(\alpha), \beta xY1(\alpha))}\ \underline{(\phi_1\ (\alpha), \beta x\varphi_1(\alpha))}$$

of the single point on the elliptic curve E and the operation information indicating the doubling,

the transforming step performs the coordinate transformation on the acquired affine coordinates of the single point to generate Jacobian coordinates

$$(X1(\alpha) : Y1(\alpha) : \beta xZ1(\alpha))$$

of the single point, and

the operating step computes

$$S(\alpha) = 4xX1(\alpha)xY1(\alpha)\ \{\ 2$$

$$M(\alpha) = 3xX1(\alpha)\ \{\ 2 + axZ1(\alpha)\ \{\ 4xf(\alpha)\ \{\ 2$$

$$T(\alpha) = -2xS(\alpha) + M(\alpha)\ \{\ 2$$

and computes

$$X3(\alpha) = T(\alpha)$$

$$Y3(\alpha) = -8xY1(\alpha) \{ 4+M(\alpha)x(S(\alpha) - T(\alpha))$$

$$Z3(\alpha) = 2xY1(\alpha)xZ1(\alpha)$$

to obtain Jacobian coordinates $(X3(\alpha) : Y3(\alpha) : \beta xZ3(\alpha))$ of the point on the elliptic curve E.

29. (Currently Amended) The storage medium of Claim 26,

wherein the acquiring step

(a) in the first case acquires affine coordinates

$$\cancel{(X1(\alpha), \beta xY1(\alpha))}\ \underline{(\phi_1(\alpha), \beta x\varphi_1(\alpha))}$$

$$\cancel{(X2(\alpha), \beta xY2(\alpha))}\ \underline{(\phi_2(\alpha), \beta x\varphi_2(\alpha))}$$

of the two different points on the elliptic curve E and the operation information indicating the addition, and

(b) in the second case acquires affine coordinates

$$\cancel{(X1(\alpha), \beta xY1(\alpha))}\ \underline{(\phi_1(\alpha), \beta x\varphi_1(\alpha))}$$

of the single point on the elliptic curve E and the operation information indicating the doubling,

wherein the transforming step

(a) in the first case performs the coordinate transformation on the acquired affine coordinates of the two different points to generate Jacobian coordinates

$$(X1(\alpha) : Y1(\alpha) : \beta xZ1(\alpha))$$

$$(X2(\alpha) : Y2(\alpha) : \beta xZ2(\alpha))$$

of the two different points, and

(b) in the second case performs the coordinate transformation on the acquired affine coordinates of the single point to generate Jacobian coordinates

$$(X1(\alpha) :Y1(\alpha) :\beta xZ1(\alpha))$$

of the single point, and

wherein the operating step

(a) in the first case computes

$$U1(\alpha) =X1(\alpha)xZ2(\alpha) \{ 2$$

$$U2(\alpha) =X2(\alpha)xZ1(\alpha) \{ 2$$

$$S1(\alpha) =Y1(\alpha)xZ2(\alpha) \{ 3$$

$$S2(\alpha) =Y2(\alpha)xZ1(\alpha) \{ 3$$

$$H(\alpha) =U2(\alpha) -U1(\alpha)$$

$$r(\alpha) =S2(\alpha) -S1(\alpha)$$

and computes

$$X3(\alpha) =-H(\alpha) \{ 3-2xU1(\alpha)xH(\alpha) \{ 2+r(\alpha) \{ 2$$

$$Y3(\alpha) =-S1(\alpha)xH(\alpha) \{ 3+r(\alpha)x(U1(\alpha)xH(\alpha) \{ 2-X3(\alpha))$$

$$Z3(\alpha) =Z1(\alpha)xZ2(\alpha)xH(\alpha)$$

to obtain Jacobian coordinates $(X3(\alpha) :Y3(\alpha) :\beta xZ3 (\alpha))$ of the point on the elliptic curve E, and

(b) in the second case computes

$$S(\alpha) =4xX1(\alpha)xY1(\alpha) \{ 2$$

$$M(\alpha) =3xX1(\alpha) \{ 2+axZ1(\alpha) \{ 4xf(\alpha) \{ 2$$

$$T(\alpha) =-2xS(\alpha) +M(\alpha) \{ 2$$

and computes

$$X3(\alpha) = T(\alpha)$$

$$Y3(\alpha) = -8xY1(\alpha) \{ 4+M(\alpha)\, x(S(\alpha) - T(\alpha))$$

$$Z3(\alpha) = 2xY1(\alpha)xZ1(\alpha)$$

to obtain the Jacobian coordinates $(X3(\alpha) : Y3(\alpha) : \beta xZ3(\alpha))$ of the point on the elliptic curve E.

30-33. (Cancelled)